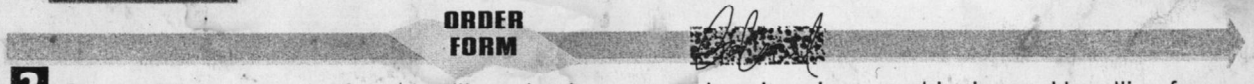
How Financial Transactions Work on the Internet

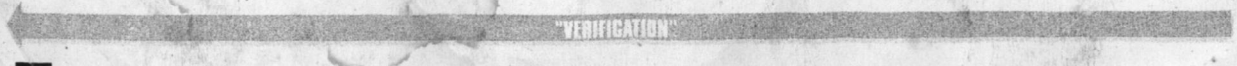
1 Gabriel browses through an electronic catalog on a Web site and he decides to buy a camcorder. To use the Secure Electronic Transaction protocol (SET) to pay for it, he will need a credit card from a participating bank and a unique "electronic signature" for his computer; this will verify that he is making the purchase, not an impostor. (In SET, everyone involved in the transaction needs electronic signatures identifying them.) SET also uses public-key encryption technology to encrypt all the information sent between everyone involved in the transaction.



2 Gabriel fills out an order form detailing what he wants to buy, its price, any shipping and handling fees, and taxes. He then selects the method he wants to use to pay. In this case, he decides to pay electronically over the Internet. At this point, he doesn't send his precise credit card number, but instead indicates which credit card he wants to use. The information he sends includes his electronic signature so the merchant can verify it is really Gabriel who wants to do the ordering.

3 The merchant receives the order form from Gabriel. The merchant's software creates a unique transaction identifier so the transaction can be identified and tracked. The merchant sends this identifier back to Gabriel along with two "electronic certificates," which are required to complete the transaction for his specific bank card. One certificate identifies the merchant and the other certificate identifies a specific *payment gateway*—an electronic gateway to the banking system that processes online payments.

4 Gabriel's software receives the electronic certificates and uses them to create Order Information (OI) and Payment Instructions (PI). It encrypts these messages and includes Gabriel's electronic signature in them. The OI and the PI are then sent back to the merchant.



5 The merchant's software decrypts Gabriel's OI and uses the electronic signature that Gabriel sent to verify that the order is from him. The merchant sends verification to Gabriel that the order has been made.

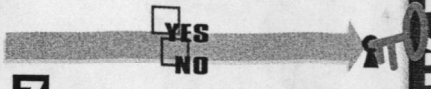
6 The merchant's software creates an authorization request for payment and includes with the merchant's digital signature the transaction identifier and the PI received from Gabriel. He encrypts all of it and sends the encrypted request to the payment gateway.

8 When the bank responds that the payment can be made, the payment gateway creates, digitally signs, and encrypts an authorization message, which is sent to the merchant. The merchant's software decrypts the message and uses the digital signature to verify that it came from the payment gateway. Assured of payment, the merchant now ships the camcorder to Gabriel.

9 Some time after the transaction has been completed, the merchant requests payment from the bank. The merchant's software creates a *capture request*, which includes the amount of the transaction, the transaction identifier, a digital signature, and other information about the transaction. The information is encrypted and sent to the payment gateway.

11 The merchant software decrypts the authorization and verifies that it is from the payment gateway. The software then stores the authorization that will be used to reconcile the credit card payment routinely when it is received from the bank.

PAYMENT GATEWAY PAYMENT GATEWAY PAY



7 The payment gateway decrypts the messages and uses the merchant's digital signature to verify that the message is from the merchant. By examining the PI, it verifies that they have come from Gabriel. The payment gateway then uses a bank card payment system to send an authorization request to the bank that issued Gabriel his bank card, asking if the purchase can be made.

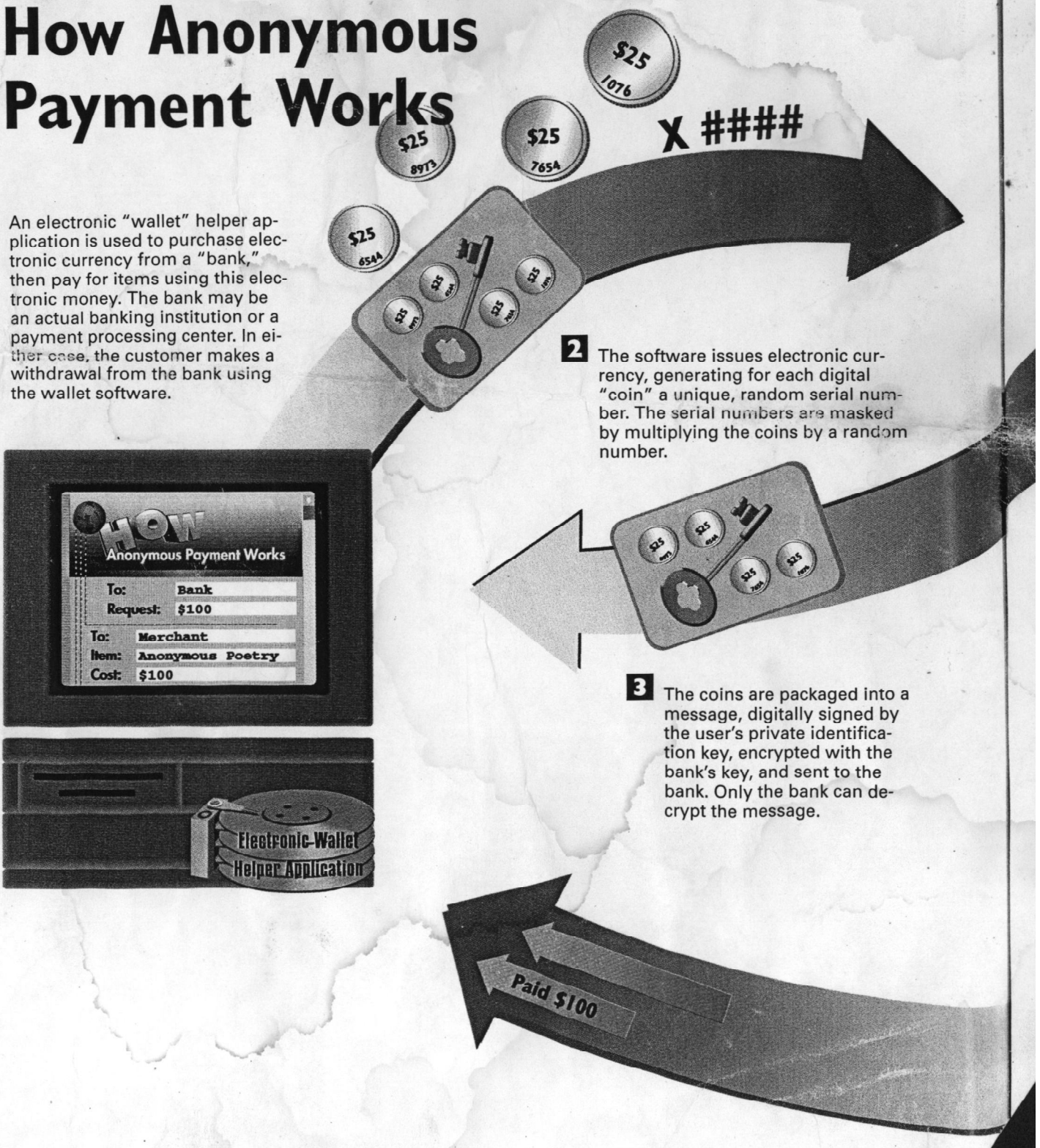
10 The payment gateway decrypts the capture request and uses the digital signature to verify it is from the merchant. It sends a request for payment to the bank, using the bank card payment system. It receives a message authorizing payment, encrypts the message, and then sends the authorization to the merchant.

BANK BANK BANK BANK BANK BANK BANK BA

LEGEND

- Internet
- ORDER FORM — Order form
- Gabriel's digital signature
- Merchant digital signature
- Payment gateway electronic signature
- ID — Unique transaction identifier
- 101100 — Merchant electronic certificate
- 101010 — Payment gateway electronic certificate
- Encryption key
- 411 — Order information
- $ — Payment/instructions
- YES / NO — Authorization request
- YES — Authorization message
- CAPTURE REQUEST — Capture request

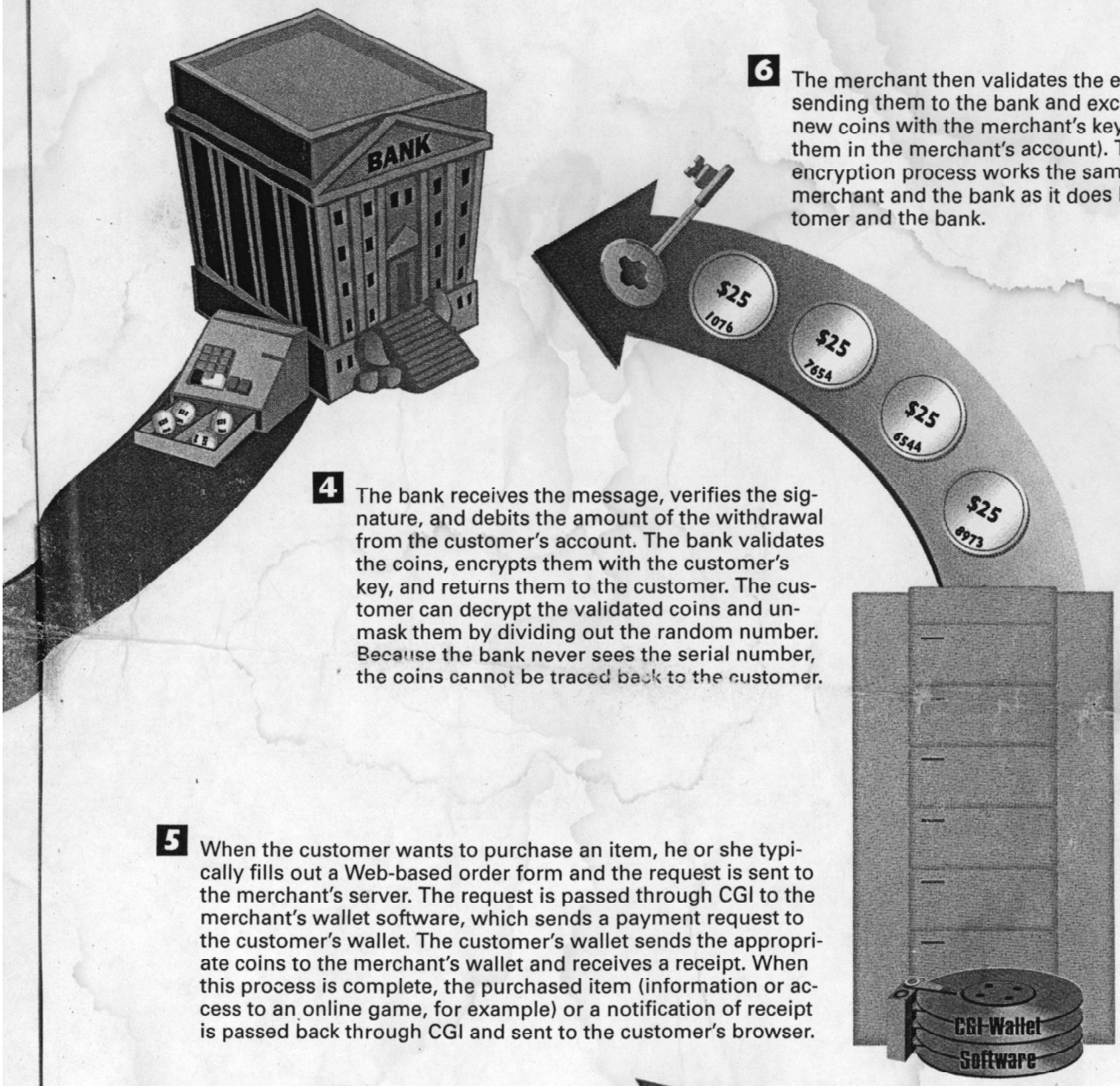
How Anonymous Payment Works



1 An electronic "wallet" helper application is used to purchase electronic currency from a "bank," then pay for items using this electronic money. The bank may be an actual banking institution or a payment processing center. In either case, the customer makes a withdrawal from the bank using the wallet software.

2 The software issues electronic currency, generating for each digital "coin" a unique, random serial number. The serial numbers are masked by multiplying the coins by a random number.

3 The coins are packaged into a message, digitally signed by the user's private identification key, encrypted with the bank's key, and sent to the bank. Only the bank can decrypt the message.

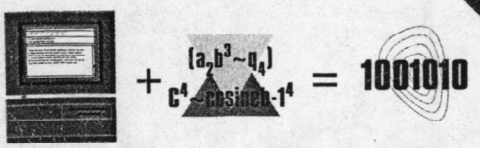


6 The merchant then validates the electronic coins by sending them to the bank and exchanging them for new coins with the merchant's key (or by depositing them in the merchant's account). The masking and encryption process works the same between the merchant and the bank as it does between the customer and the bank.

4 The bank receives the message, verifies the signature, and debits the amount of the withdrawal from the customer's account. The bank validates the coins, encrypts them with the customer's key, and returns them to the customer. The customer can decrypt the validated coins and unmask them by dividing out the random number. Because the bank never sees the serial number, the coins cannot be traced back to the customer.

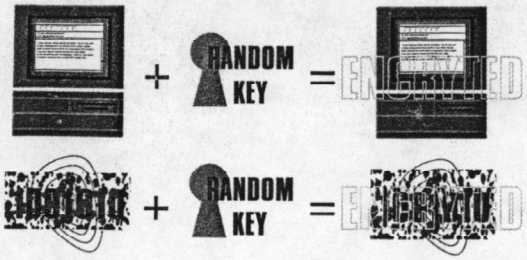
5 When the customer wants to purchase an item, he or she typically fills out a Web-based order form and the request is sent to the merchant's server. The request is passed through CGI to the merchant's wallet software, which sends a payment request to the customer's wallet. The customer's wallet sends the appropriate coins to the merchant's wallet and receives a receipt. When this process is complete, the purchased item (information or access to an online game, for example) or a notification of receipt is passed back through CGI and sent to the customer's browser.

How Cryptosystems Work



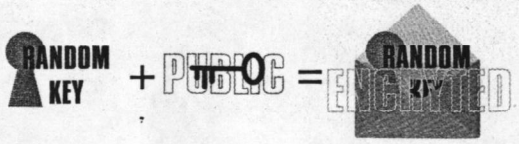
1 Gabriel wants to send a confidential message over the Internet to Mia. Mia will need some way to decrypt the message as well as a way to guarantee that Gabriel, and not an imposter, has actually sent the message. First, Gabriel runs his message through an algorithm called a *hash function*. This produces a number known as the *message digest*. The message digest acts as a sort of "digital fingerprint" that Mia will use to ensure that no one has altered the message.

2 Gabriel now uses his private key to encrypt the message digest. This produces a unique digital signature that only he, with his private key, could have created.

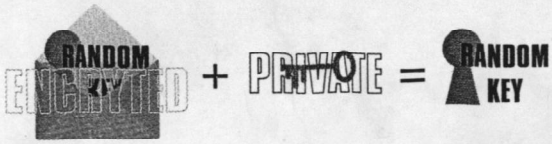


3 Gabriel generates a new random key. He uses this key to encrypt his original message and his digital signature. Mia will need a copy of this random key to decrypt Gabriel's message. This random key is the only key in the world that can decrypt the message—and at this point only Gabriel has the key.

4 Gabriel encrypts this new random key with Mia's public key. This encrypted random key is referred to as the *digital envelope*. Only Mia will be able to decrypt the random key because it was encrypted with her public key, so only her private key can decrypt it.



5 Gabriel sends a message over the Internet to Mia that is composed of several parts: the encrypted confidential message, the encrypted digital signature, and the encrypted digital envelope.

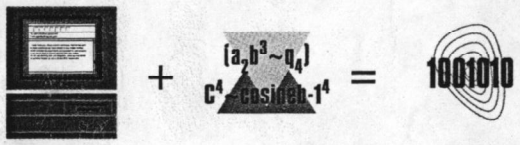


6 Mia gets the message. She decrypts the digital envelope with her private key and out of it gets the random key that Gabriel used to encrypt the message.

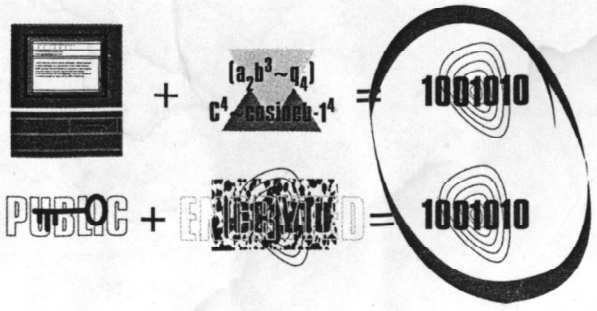
7 Mia uses the random key to decrypt Gabriel's message. She can now read the confidential message that he sent to her. However, she can't yet be sure that the message hasn't been altered en route to her or that Gabriel was definitely the sender.

8 Mia now uses the random key and Gabriel's public key to decrypt his encrypted digital signature. When she does this, she gets his message digest, the message's "digital fingerprint."

9 Mia will use this message digest to see whether Gabriel indeed sent the message and that it was not altered in any way. She takes the message that she decrypted and runs it through the same algorithm—the hash function—that Gabriel ran the message through. This will produce a new message digest.



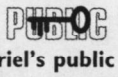
10 Mia compares the message digest that she calculated to the one that she got out of Gabriel's digital signature. If the two match precisely, she can be sure that Gabriel signed the message and that it was not altered after he composed it. If they don't match, then she knows that either he didn't compose the message, or that someone altered the message after he wrote it.



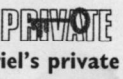

Original message


Hash function

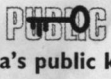
Message digest



Gabriel's public key



Gabriel's private key



Mia's public key

Mia's private key


Digital signature

Random key

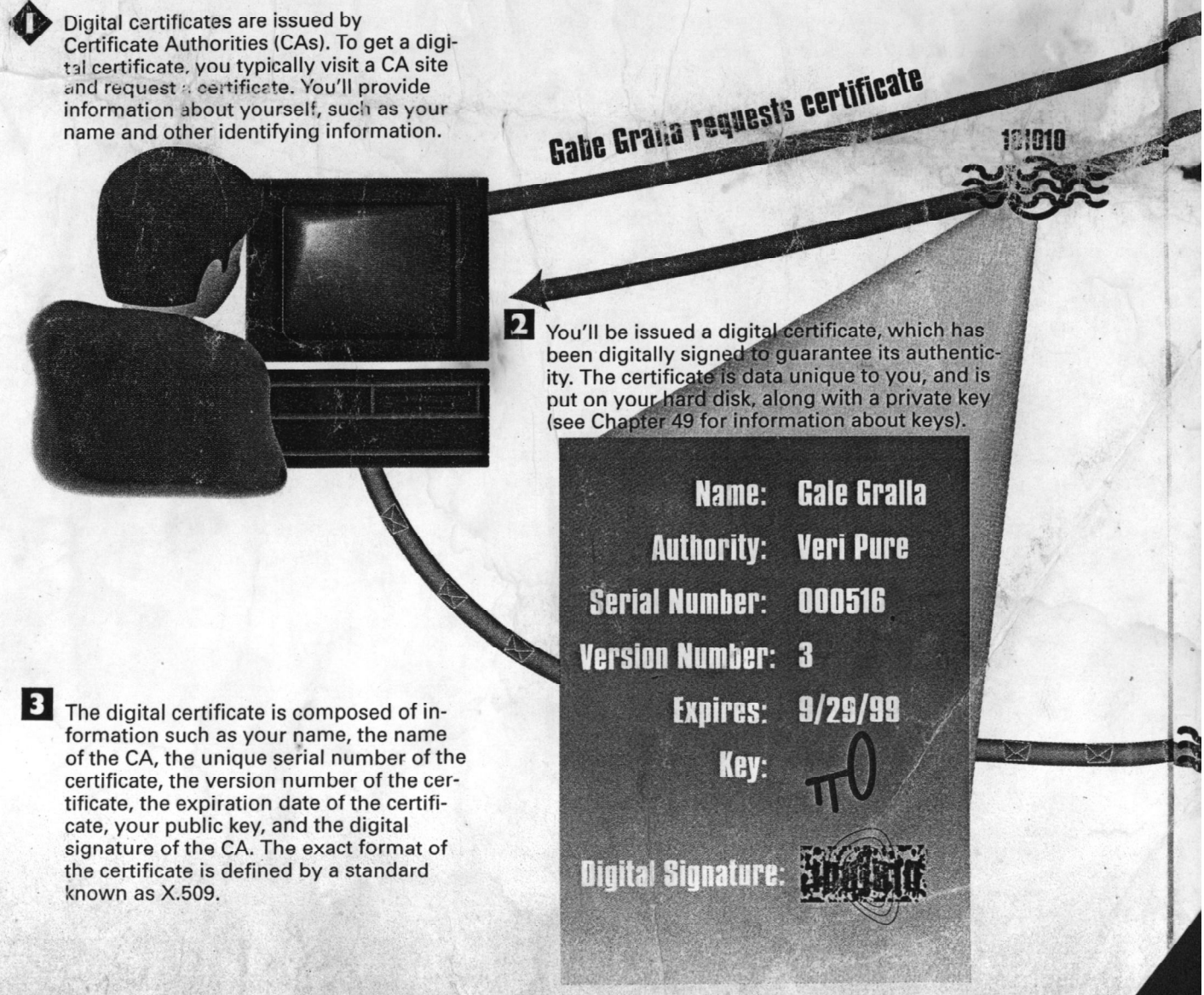
Encrypted message


Encrypted digital signature

Encrypted random key (digital envelope)

How Digital Certificates Ensure Internet Security

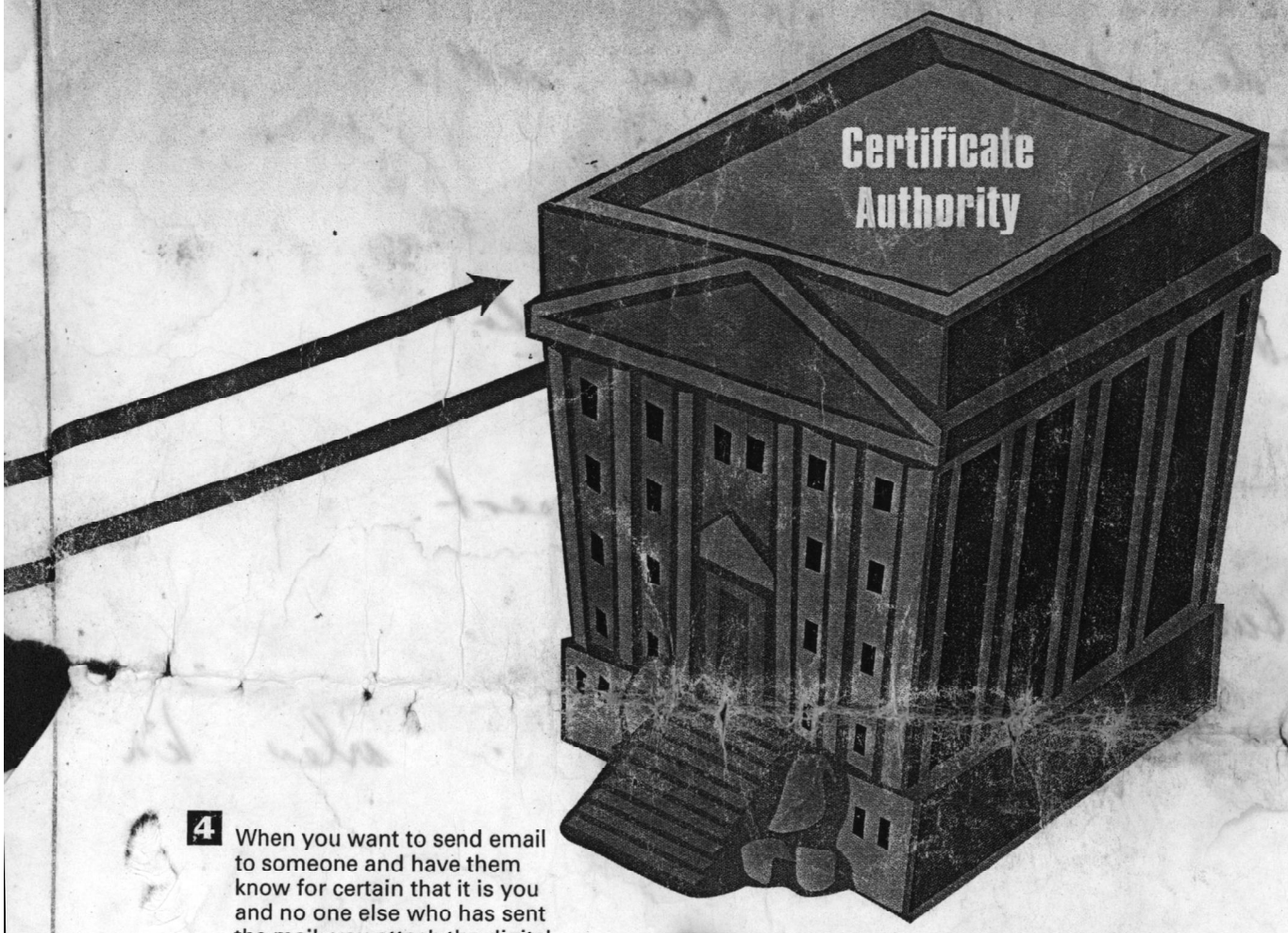
A digital certificate is used to guarantee that the person who sends information or email over the Internet or who makes a financial transaction really is who he says he is. This illustration shows how a digital certificate would be used to guarantee that the person sending an email is being truthful about his identity.



1 Digital certificates are issued by Certificate Authorities (CAs). To get a digital certificate, you typically visit a CA site and request a certificate. You'll provide information about yourself, such as your name and other identifying information.

2 You'll be issued a digital certificate, which has been digitally signed to guarantee its authenticity. The certificate is data unique to you, and is put on your hard disk, along with a private key (see Chapter 49 for information about keys).

3 The digital certificate is composed of information such as your name, the name of the CA, the unique serial number of the certificate, the version number of the certificate, the expiration date of the certificate, your public key, and the digital signature of the CA. The exact format of the certificate is defined by a standard known as X.509.



4 When you want to send email to someone and have them know for certain that it is you and no one else who has sent the mail, you attach the digital certificate to your email message. One of the things that the certificate does is sign the message with a private key that you were given as part of the digital certificate.

5 The person you're sending email to gets your digital certificate along with your email. The key is used to read the private key's signature. That signature matches information found in the digital certificate, and so the receiver is assured that the message really came from you.